TO: USPTO

RECEIVED
CENTRAL FAX CENTER
NOV 13 2006

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

		Phone Number	Fax Number
Date:	November 13, 2006		
To:	Examiner Pyzocha		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAi1P459/01.021.01

App. No: 09/854,492

Total Number of Pages Being Transmitted, Including Cover Sheet: 44

Message:

Please deliver to Examiner Pyzocha.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

November 13, 2006

RECEIVED
CENTRAL FAX CENTER
NOV 13 2006

Practitioner's Docket No. NA1P459/01.021.01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: D. Wolff et al.

Application No.: 09/854,492
Filed: 05/15/2001
Group No.: 2137
Examiner: Pyzocha, M.
For: EVENT REPORTING BETWEEN A REPORTING COMPUTER AND A RECEIVING COMPUTER

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 07/11/2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed 08/14/06.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. ______________ **(mandatory)**

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 11/13/2006

Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

PAGE 2/44 * RCVD AT 11/13/2006 3:14:12 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/13 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):10-34

11/15/2006 EFLORES 00000048 501351 09854492
02 FC:1252 450.00 DA

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for two months:

Fee:	$450.00

If an additional extension of time is required, please consider this a petition therefor.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$450.00
TOTAL FEE DUE	**$950.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $950.00 to Deposit Account No. 50-1351 (Order No. NAI1P459).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P459).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

RECEIVED
CENTRAL FAX CENTER
NOV 13 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Wolff et al.	Group Art Unit: 2137
Application No. 09/854,492	Examiner: Pyzocha, Michael J.
Filed: May 15, 2001	Date: November 13, 2006
For: EVENT REPORTING BETWEEN A REPORTING COMPUTER AND A RECEIVING COMPUTER	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 07/11/2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed 08/14/06.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-6, 8-17, 19-28, 30-39, 41-50, 52-61, and 63-74

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-6, 8-17, 19-28, 30-39, 41-50, 52-61, and 63-74
3. Claims allowed: None
4. Claims rejected: 1-6, 8-17, 19-28, 30-39, 41-50, 52-61, and 63-74
5. Claims cancelled: 7, 18, 29, 40, 51, and 62

C. CLAIMS ON APPEAL

The claims on appeal are: 1-6, 8-17, 19-28, 30-39, 41-50, 52-61, and 63-74

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1 and 2, a computer program product is provided which comprises a computer program operable to control a reporting computer to report the occurrence of an event to a receiving computer is provided. In use, report generating logic is operable to generate report data (e.g. see item 26 of Figure 2, etc.) identifying the reporting computer (e.g. see item 2 of Figure 1, etc.) and the event. Further, data retrieving logic is operable to fetch requested data from the receiving computer (e.g. see item 6 of Figure 1, etc.) to the reporting computer upon a request of the reporting computer. In addition, report sending logic is operable to send the report data (e.g. see item 26 of Figure 2, etc.) from the reporting computer (e.g. see item 2 of Figure 1, etc.) to the receiving computer (e.g. see item 6 of Figure 1, etc.) during the fetch of the requested data. The data retrieving logic and the report sending logic use an internet URL (e.g. see item 20 of Figure 2, etc.) to specify the requested data to the receiving computer. The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer. See, for example, page 5, line 30 – page 7, line 28 et al.

With respect to a summary of Claim 12, as shown in Figures 1 and 2, a computer program product is provided which comprises a computer program operable to control a receiving computer to receive a report of an occurrence of an event from a reporting computer. In use, data request receiving logic is operable to receive a request for requested data from the reporting computer (e.g. see item 2 of Figure 1, etc.). Further, data providing logic is operable to provide the requested data to the reporting computer (e.g. see item 2 of Figure 1, etc.). In addition, report receiving logic is operable to receive report data (e.g. see item 26 of Figure 2, etc.) identifying the reporting computer (e.g. see item 2 of Figure 1, etc.) and the event from the reporting computer during the providing of the requested data to the reporting computer. The data retrieving logic and the report sending logic use an internet URL (e.g. see item 20 of Figure 2, etc.) to specify the requested data to the receiving computer (e.g. see item 6 of Figure 1, etc.). The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer (e.g. see item 6 of Figure 1, etc.). See, for example, page 5, line 30 – page 7, line 28 et al.

With respect to a summary of Claim 23, as shown in Figures 1 and 2, a method of controlling a reporting computer to report an occurrence of an event to a receiving computer is provided. In use, report data (e.g. see item 26 of Figure 2, etc.) identifying the reporting computer (e.g. see item 2 of Figure 1, etc.) and the event is generated. Further, requested data is fetched from the receiving computer (e.g. see item 6 of Figure 1, etc.) to the reporting computer upon a request of the reporting computer. In addition, the report data (e.g. see item 26 of Figure 2, etc.) is sent from the reporting computer to the receiving computer during fetching of the requested data. An internet URL (e.g. see item 20 of Figure 2, etc.) is used to specify the requested data to the receiving computer. The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer. See, for example, page 5, line 30 – page 7, line 28 et al.

With respect to a summary of Claim 34, as shown in Figures 1 and 2, a method of controlling a receiving computer to receive a report of an occurrence of an event from a reporting computer is provided. In use, a request for requested data is received from the reporting computer (e.g. see item 2 of Figure 1, etc.). Further, the requested data is provided to the reporting computer. In addition, report data (e.g. see item 26 of Figure 2, etc.) is received that identifies the reporting computer and the event from the reporting computer during providing of the requested data to the reporting computer. An internet URL (e.g. see item 20 of Figure 2, etc.) is used to specify the requested data to the receiving computer (e.g. see item 6 of Figure 1, etc.). The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer. See, for example, page 5, line 30 – page 7, line 28 et al.

With respect to a summary of Claim 45, as shown in Figures 1 and 2, a reporting computer operable to report occurrence of an event to a receiving computer is provided. In use, a report generator is operable to generate report data (e.g. see item 26 of Figure 2, etc.) identifying the reporting computer (e.g. see item 2 of Figure 1, etc.) and the event. Further, a data retriever is operable to fetch requested data from the receiving computer (e.g. see item 6 of Figure 1, etc.) to the reporting computer upon a request of the reporting computer. In addition, a report sender is operable to send the report data (e.g. see item 26 of Figure 2, etc.) from the reporting computer to the receiving computer during the fetch of the requested data. An internet URL (e.g. see item 20

of Figure 2, etc.) is used to specify the requested data to the receiving computer. The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer (see, for example, page 5, line 30 – page 7, line 28 et al.).

With respect to a summary of Claim 56, as shown in Figures 1 and 2, a receiving computer operable to receive a report of occurrence of an event from a reporting computer is provided. In use, a data request receiver is operable to receive a request for requested data from the reporting computer (e.g. see item 2 of Figure 1, etc.). Further, a data provider is operable to provide the requested data to the reporting computer. In addition, a report receiver is operable to receive report data (e.g. see item 26 of Figure 2, etc.) identifying the reporting computer and the event from the reporting computer during providing of the requested data to the reporting computer. An internet URL (e.g. see item 20 of Figure 2, etc.) is used to specify the requested data to the receiving computer (e.g. see item 6 of Figure 1, etc.). The internet URL specifying the requested data also contains the report data (e.g. see item 26 of Figure 2, etc.) to be sent to the receiving computer. See, for example, page 5, line 30 – page 7, line 28 et al.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-6, 8, 10-17, 19, 21-28, 30, 32-39, 41, 43-50, 52, 54-61, 63, 65-66, and 72-74 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), and further in view of Graham ("URLs for HTTP Servers").

Issue # 2: The Examiner has rejected Claims 9, 20, 31, 42, 53, and 64 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), and further in view of Menezes et al. ("Handbook of Applied Cryptography").

Issue # 3: The Examiner has rejected Claim 67 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), in view of Norton ("Norton Antivirus Corporate Edition Implementation Guide"), and further in view of Grundy (U.S. Patent No. 5,291,598).

Issue # 4: The Examiner has rejected Claims 68-69 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), and further in view of Williams (U.S. Publication No. 2002/0138435).

Issue # 5: The Examiner has rejected Claims 70-71 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S.

Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), and further in view of Cox (U.S. Patent No. 6,842,861).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-6, 8, 10-17, 19, 21-28, 30, 32-39, 41, 43-50, 52, 54-61, 63, 65-66, and 72-74 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), and further in view of Graham ("URLs for HTTP Servers").

Group #1: Claims 1-3, 10-14, 21-25, 32-36, 43-47, 54-58, 65-66, and 72-74

With respect to independent Claims 1, 12, 23, 34, 45, and 56, the Examiner has relied on section 8.1.1 in Graham to make a prior art showing of appellant's claimed technique "wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that such excerpt only teaches a URL that includes (1) the directory to a program/script and (2) the search parameters for the program/script to utilize when performing a search. Appellant emphasizes the URL example shown in section 8.1.1 as follows: <u>http://some.site.edu/cgi-bin/foo?arg1+arg2+arg3</u>. As shown in Graham, such URL only contains the directory (i.e. <u>http://some.site.edu/cgi-bin/foo</u>), and the parameters (i.e. arg1+arg2+arg3). Appellant, on the other hand, claims that the "internet URL also contain[s] said <u>report data</u> to be sent to said receiving computer" (emphasis added), as claimed. Clearly, Graham's disclosed directory and parameters do not meet appellant's claimed report data, especially when read in context, namely that the "report data identif[ies] said <u>reporting computer</u> and said <u>event</u>" (see the independent claims), in the context as claimed by appellant.

In the Office Action mailed 04/11/2006, the Examiner has argued that "Graham is relied upon to show that a URL [m]a[y] send data and this data is what is defined as the requested data in the combination of Symantec and Chen et al."

In response, appellant respectfully asserts that the combination of Symantec, Chen, Brown and Graham et al. fails to disclose appellant's claimed "sending said report data from said reporting computer to said receiving computer during fetching of said requested data," "wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer," as claimed.

Specifically, the Examiner has relied upon Col. 7, lines 33-45 in Chen to make a prior art showing of appellant's claimed "sending said report data from said reporting computer to said receiving computer during fetching of said requested data," as claimed.

Appellant respectfully asserts that Chen merely discloses that, "[a]fter receipt of the virus detection object, in step 220 the virus detection object is executed by the client 300 and in step 225 the <u>results of virus detection object execution are transmitted to the virus detection server</u> 400 which receives the results and in step 230 <u>produces an additional virus detection based upon the result</u> of the execution of the first virus detection object" (emphasis added). Clearly, Chen's disclosure that the additional virus detection object is produced based on the result of the execution (along with the disclosure of the remaining references) fails to even suggest "<u>sending said report data</u> from said reporting computer to said receiving computer <u>**during fetching of said requested data**</u>" (emphasis added), as claimed by appellant. Since Chen discloses sending the result, and <u>then</u> receiving the additional virus detection, Chen fails to even suggest appellant's claimed "sending said report data ... <u>during</u> fetching of said requested data" (emphasis added), as claimed.

In addition, it appears that the Examiner has further relied upon page 2 in Brown to make a prior art showing of appellant's claimed "sending said report data ... during fetching of said requested data," as claimed.

Appellant points out that page 2 of Brown discloses that, with Full Duplex, "[d]ata can travel in both directions simultaneously [and] [t]here is no need to switch from transmit to receive mode like in half duplex" (emphasis added). However, page 1 of Brown discloses that "you can think of Internet surfing as being half-duplex, as a user issues a **request for a web document**, then that document is downloaded and displayed **before** the user issues another **request**" (emphasis added). Clearly, Brown's disclosure of Internet requests for a web document being half-duplex fails to meet and even *teaches away* from appellant's claimed "sending said report data ... **during** fetching of said requested data" (emphasis added), as claimed.

To this end, even when the Examiner's proposed combination is taken into account in its entirety, the appellant's claim language is still not met, as noted above. Further, appellant respectfully asserts that it is improper to combine references where the references *teach away*. *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983).

Still with respect to the independent claims, and particularly appellant's claimed technique "wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL also containing said report data to be sent to said receiving computer" (see this or similar, but not necessarily identical language in the independent claims), appellant respectfully asserts that Graham merely discloses that "[t]he HTTP protocol support[s] the passing of arguments to the server" where "[t]he general format is to postpend the arguments to the URL, separated from the URL by a question mark (?)."

However, merely passing arguments to the server by postpending the arguments to the URL (along with the disclosure of the remaining references), as in Graham, fails to even suggest a technique "wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer" (emphasis added), as claimed by appellant. Clearly, the mere disclosure that "these programs/scripts can in turn act on the arguments and **return** information, documents, etc. to the browser" (emphasis added - along with the disclosure of the remaining references) fails to even suggest that "said requested data also contain[s] said report data," where

the "report data identif[ies] said <u>reporting computer</u> and said <u>event</u>" (emphasis added), as claimed by appellant. Again, when the Examiner's proposed combination is taken into account in its entirety, the claimed invention is still not met.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claims 4, 15, 26, 37, 48, and 59

With respect to Claims 4, 15, 26, 37, 48, and 59, the Examiner has relied on pages 13 and 18 in Symantec to make a prior art showing of appellant's claimed technique "wherein said requested data is a description of said event."

Appellant respectfully asserts that such excerpts from Symantec only teach that the Symantec System Center provides alerting, logging and data export and activating tasks, and that virus update files and product updates can be retrieved from a master primary server. Clearly, such teachings do not even suggest a "<u>description</u> of said event" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/11/2006, the Examiner has argued that "the alert described on pages 13, 18, and 73 of Symantec clearly describe an event, by showing when, where, and what happened."

Appellant respectfully asserts that page 73 of Symantec merely discloses an "Alert Log [which] displays a list of alerts with information about each alert: Alert Name, Source, Computer, Date, Time, Severity." However, merely listing information about the alert fails to even suggest a technique "wherein said requested data is a description of said event" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #3: Claims 5, 16, 27, 38, 49, and 60

With respect to Claims 5, 16, 27, 38, 49, and 60, the Examiner has relied on pages 18 and 73 in Symantec to make a prior art showing of appellant's claimed technique "wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus."

First, appellant respectfully asserts that Symantec does not teach a description of a computer virus, as claimed by appellant, for the reasons noted above with respect to Issue #1, Group #2. Second, it seems the Examiner has attempted to show that Symantec discloses a detection of a computer virus, and that Symantec provides a description of a computer virus, without taking into account the context of appellant's claim language. In particular, appellant claims that "said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus" (emphasis added) where, "report data identif[ies]...said event" in the manner as claimed by appellant (see the independent claims for context).

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #4: Claims 6, 17, 28, 39, 50, and 61

With respect to Claims 6, 17, 28, 39, 50, and 61, the Examiner has again relied on pages 18 and 73 in Symantec to make a prior art showing of appellant's claimed technique "wherein said event

is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses." For substantially the same reasons as argued above with respect to Issue #1, Group #3, appellant respectfully asserts that Symantec fails to teach appellant's specific claim language <u>when read in context</u>.

In the Office Action mailed 04/11/2006, the Examiner has argued that "Symantec is relied upon for its teaching of the report data with the report data describing an event, by showing when, where, and what happened and Chen et al teaches sending the requested report data."

Appellant respectfully asserts that Col. 7, lines 33-45 of Chen merely discloses that "results of virus detection object execution are transmitted to the <u>virus detection server</u> 400 which receives the results and in step 230 <u>produces an additional virus detection</u> <u>based upon the result</u> of the execution of the first virus detection object" (emphasis added). Clearly, the mere disclosure that the virus detection server produces an additional virus detection based upon the result fails to even suggest that "said <u>requested data</u> is an <u>updated set of computer virus detecting data</u> for use in detecting computer viruses" (see Claim 6 et al. – emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #5: Claims 8, 19, 30, 41, 52, and 63

With respect to Claims 8, 19, 30, 41, 52, and 63, the Examiner has relied on the Figure on page 73 of Symantec to make a prior art showing of appellant's claimed technique "wherein said reporting computer collates report data specifying one or more events that is sent together from said reporting computer to said receiving computer during said fetch of said requested data."

Appellant respectfully asserts that such figure only shows a list of alerts. Clearly, a list of alerts that each show the type of event discovered and the computer from which said event occurred does not meet <u>all</u> of appellant's claim language, namely that "said reporting computer collates report data specifying one or more events <u>that is sent together from said reporting computer to said receiving computer during said fetch of said requested data</u>" (emphasis added), as claimed

by appellant. In fact, appellant notes that the log shown on page 73 of Symantec is associated with a specific server and that a copy is merely displayed when requested by a local console, but not that collated report data "is sent…during said fetch of said requested data," as claimed by appellant.

In the Office Action mailed 04/11/2006, the Examiner has argued that "Symantec teaches generating a list of all alerts generated by the network computers" and that "[i]n combination these alerts were collected during the fetch of the requested data as taught by Chen et al." However, appellant respectfully asserts that Col. 7, lines 33-45 in Chen merely discloses that the "virus detection object is executed by the client 300 and in step 225 the results of virus detection object execution are transmitted to the virus detection server" (emphasis added).

Clearly, transmitting results of the virus detection object execution, as in Chen, fails to even suggest that "said reporting computer collates report data specifying one or more **events** that is sent together from said reporting computer to said receiving computer during said fetch of said requested data" (emphasis added), as claimed by appellant. In addition, Symantec teaches that "[e]ach server stores its own copy of the Alert Log locally" and that "[w]hen you select a server an[d] view its alert log, you're actually retrieving a copy of that server's Alert Log to your local console" (emphasis added). Clearly, disclosing the server has a copy which is retrieved to the local console upon viewing, as in Chen, fails to even suggest that "said reporting computer collates report data specifying one or more events that is **sent** together from said reporting computer to said receiving computer **during** said fetch of said requested data" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 2:

The Examiner has rejected Claims 9, 20, 31, 42, 53, and 64 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of

Graham ("URLs for HTTP Servers") and further in view of Menezes et al. ("Handbook of Applied Cryptography").

Group #1: Claims 9, 20, 31, 42, 53, and 64

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued above with respect to Issue #1, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 3:

The Examiner has rejected Claim 67 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), in view of Norton ("Norton Antivirus Corporate Edition Implementation Guide"), and further in view of Grundy (U.S. Patent No. 5,291,598).

Group #1: Claim 67

With respect to Claim 67, the Examiner has relied on page 73 of the Symantec reference, in addition to pages 286-287 of the Norton reference, and Col. 18, lines 45-57 of the Grundy reference to make a prior art showing of appellant's claimed technique "wherein said report data includes: a MAC address identifying a network card of said reporting computer; a date of said event; a time of said event; an identifier of a computer program used by said reporting computer to detect said event; an identifier of a version of a computer program used by said reporting computer to detect said event; an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event; an identifier of an event type detected by said reporting computer; an action taken by said reporting computer upon detection of said event; and a checksum of a file that triggered said event."

Appellant respectfully asserts that the excerpt from Symantec relied upon by the Examiner merely discloses that "[t]he Alert Log displays a list of alerts with this information about each alert: Alert Name, Source, Computer, Date, Time, [and] Severity." However, merely disclosing that the alert log lists information on each alert simply fails to even suggest a technique "wherein said report data includes: a MAC address identifying a network card of said reporting computer; a date of said event; a time of said event; an identifier of a computer program used by said reporting computer to detect said event; an identifier of a version of a computer program used by said reporting computer to detect said event; an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event; an identifier of an event type detected by said reporting computer; an action taken by said reporting computer upon detection of said event; and a checksum of a file that triggered said event" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpt from Norton cited by the Examiner merely discloses "view[ing] virus activity and scanning on your network" as well as "histories for selected server groups, for a single server group, or for selected computers within a server group." Further, Norton discloses that "[i]f you select a server group, Virus History lists information about viruses detected on all computers throughout the server group." In addition, Norton discloses a Virus History, which "shows...the name and location of the infected file, the name of the infected computer, the primary and secondary actions that were configured for the detected virus, and what action was taken on the virus," a Virus Sweep History, a Scan History, and an Event Log, which "contains all other logged information that does not fall into the previous two categories...[such as] messages about virus definitions file or configuration changes for specific computers" (emphasis added).

However, the mere disclosure of a Virus History, a Virus Sweep History, a Scan History, and an Event Log simply fail to disclose "an identifier of a version of a computer program used by said reporting computer to detect said event" as well as "an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event" (emphasis added), as claimed by appellant. In addition, Norton's mere disclosure of an Event Log containing messages about virus definition files or configuration changes simply fails to suggest "an identifier ... used... to detect said event," in the manner as claimed by appellant.

In addition, with respect to the excerpt from Grundy relied upon by the Examiner, appellant respectfully asserts that Grundy merely teaches that "an anti-virus checksum of the host software product is calculated" which is used "to ensure that the copy of the product being registered has not been corrupted in any way" (emphasis added). Clearly, the mere disclosure of calculating an anti-virus checksum to ensure that the product being registered is not corrupted simply fails to even suggest "a checksum of a file that triggered said event" (emphasis added), as claimed by appellant.

In addition, with respect to dependent Claim 67, the Examiner has dismissed the same under Official Notice. Specifically, the Examiner has stated that it would have been obvious for one of ordinary skill in the art at the time the invention was made to use a MAC address to identify the computer, and that motivation to do so would have been that MAC addresses provide a unique identity of a computer. Appellant respectfully disagrees. In particular, appellant respectfully asserts that a MAC address is generally utilized for identifying a network card.

Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the [appellant] traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that it would have been obvious to combine Norton and Grundy with the modified Symantec, Chen et al., Brown, and Graham system because to do so would have enabled viewing the virus activity and scanning on the network and to make sure the file isn't corrupt. To the contrary, appellant respectfully asserts that it would not have been obvious to combine the Norton and Grundy references with the modified Symantec, Chen et al., Brown, and Graham system, especially in view of the vast evidence to the contrary.

For example, Grundy relates to a system for decentralized manufacturing of copy-controlled software, while Chen relate to anti-virus scanners, Symantec relates to managing anti-virus scanners, Brown relates to half-duplex and full-duplex data communications, and Graham relates to URLs for HTTP servers. To simply glean features from a system for manufacturing copy-controlled software, such as that of Grundy, and combine the same with the *non-analogous art* of an anti-virus scanner, such as that of Chen, or the *non-analogous art* of managing anti-virus scanners, such as that of Symantec, would simply be improper. In particular, copy-controlled software generates registration codes, accepts and verifies authorization codes, and determines the operational mode of the product, while anti-virus scanners detect and treat viruses. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a <u>copy-controlled software manufacturing system</u> addresses as opposed to <u>anti-virus scanners</u>, the Examiner's proposed combination is inappropriate.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest <u>all</u> of the claim limitations, as noted above.

<u>Issue # 4:</u>

The Examiner has rejected Claims 68-69 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), and further in view of Williams (U.S. Publication No. 2002/0138435).

Group #1: Claims 68-69

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued above with respect to Issue #1, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Issue # 5:

The Examiner has rejected Claims 70-71 under 35 U.S.C. 103(a) as being unpatentable over Symantec ("Symantec System Center Implementation Guide"), in view of Chen et al. (U.S. Patent No. 5,960,170), in view of Brown ("Data Communications"), in view of Graham ("URLs for HTTP Servers"), and further in view of Cox (U.S. Patent No. 6,842,861).

Group #1: Claims 70

With respect to Claim 70, the Examiner has relied on Col. 1, lines 21-39 of the Cox reference to make a prior art showing of appellant's claimed technique "wherein said report data includes an identifier of a driver triggered during said event."

Appellant respectfully asserts that the excerpt from Cox relied upon by the Examiner merely discloses that "[a] virus can infect, or become resident in almost any software component, including an application, operating system, system boot code, or device driver" (emphasis added). However, the mere disclosure that a virus can infect or become resident in a device driver simply fails to even suggest a technique "wherein said report data includes an identifier of a driver triggered during said event" (emphasis added), as claimed by appellant, or a technique "wherein said identifier of said driver is mapped to an identity of a virus that triggered said event" (emphasis added), as claimed by appellant. Clearly, the excerpt from Cox fails to even suggest "an identifier of a driver triggered during an event," in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

Group #2: Claim 71

With respect to Claim 70, the Examiner has relied on Col. 1, lines 21-39 of the Cox reference to make a prior art showing of appellant's claimed technique "wherein said identifier of said driver is mapped to an identity of a virus that triggered said event."

Appellant respectfully asserts that the excerpt from Cox relied upon by the Examiner merely discloses that "[a] virus can infect, or become resident in almost any software component, including an application, operating system, system boot code, or device driver" (emphasis added). However, the mere disclosure that a virus can infect or become resident in a device driver simply fails to even suggest a technique "wherein said identifier of said driver is mapped to an identity of a virus that triggered said event" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (previously presented) A computer program product comprising a computer program operable to control a reporting computer to report occurrence of an event to a receiving computer, said computer program comprising:

report generating logic operable to generate report data identifying said reporting computer and said event;

data retrieving logic operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

report sending logic operable to send said report data from said reporting computer to said receiving computer during said fetch of said requested data;

wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

2. (original) A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing an unwanted computer program.

3. (original) A computer program product as claimed in claim 2, wherein said unwanted computer program is a computer virus.

4. (original) A computer program product as claimed in claim 1, wherein said requested data is a description of said event.

5. (original) A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

6. (original) A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

7. (cancelled)

8. (previously presented) A computer program product as claimed in claim 1, wherein said reporting computer collates report data specifying one or more events that is sent together from said reporting computer to said receiving computer during said fetch of said requested data.

9. (original) A computer program product as claimed in claim 1, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

10. (original) A computer program product as claimed in claim 1, wherein said reporting computer and said receiving computer communicate via an internet link.

11. (original) A computer program product as claimed in claim 1, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

12. (previously presented) A computer program product comprising a computer program operable to control a receiving computer to receive a report of occurrence of an event from a reporting computer, said computer program comprising:

data request receiving logic operable to receive a request for requested data from said reporting computer;

data providing logic operable to provide said requested data to said reporting computer; and

report receiving logic operable to receive report data identifying said reporting computer and said event from said reporting computer during providing of said requested data to said reporting computer;

wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

13. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing an unwanted computer program.

14. (original) A computer program product as claimed in claim 13, wherein said unwanted computer program is a computer virus.

15. (original) A computer program product as claimed in claim 12, wherein said requested data is a description of said event.

16. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

17. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

18. (cancelled)

19. (previously presented) A computer program product as claimed in claim 12, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

20. (original) A computer program product as claimed in claim 12, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

21. (original) A computer program product as claimed in claim 12, wherein said reporting computer and said receiving computer communicate via an internet link.

22. (original) A computer program product as claimed in claim 12, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

23. (previously presented) A method of controlling a reporting computer to report occurrence of an event to a receiving computer, said method comprising the steps of:

generating report data identifying said reporting computer and said event;

fetching requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

sending said report data from said reporting computer to said receiving computer during fetching of said requested data;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

24. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing an unwanted computer program.

25. (original) A method as claimed in claim 24, wherein said unwanted computer program is a computer virus.

26. (original) A method as claimed in claim 23, wherein said requested data is a description of said event.

27. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

28. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

29. (cancelled)

30. (previously presented) A method as claimed in claim 23, wherein said reporting computer collates report data specifying one or more events that is sent together from said reporting computer to said receiving computer during fetching of said requested data.

31. (original) A method as claimed in claim 23, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

32. (original) A method as claimed in claim 23, wherein said reporting computer and said receiving computer communicate via an internet link.

33. (original) A method as claimed in claim 23, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

34. (previously presented) A method of controlling a receiving computer to receive a report of occurrence of an event from a reporting computer, said method comprising the steps of:

receiving a request for requested data from said reporting computer;

providing said requested data to said reporting computer; and

receiving report data identifying said reporting computer and said event from said reporting computer during providing of said requested data to said reporting computer;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

35. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing an unwanted computer program.

36. (original) A method as claimed in claim 35, wherein said unwanted computer program is a computer virus.

37. (original) A method as claimed in claim 34, wherein said requested data is a description of said event.

38. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

39. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

40. (cancelled)

41. (previously presented) A method as claimed in claim 34, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

42. (original) A method as claimed in claim 34, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

43. (original) A method as claimed in claim 34, wherein said reporting computer and said receiving computer communicate via an internet link.

44. (original) A method as claimed in claim 34, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

45. (previously presented) A reporting computer operable to report occurrence of an event to a receiving computer, said reporting computer comprising:

a report generator operable to generate report data identifying said reporting computer and said event;

a data retriever operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

a report sender operable to send said report data from said reporting computer to said receiving computer during said fetch of said requested data;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

46. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing an unwanted computer program.

47. (original) A reporting computer as claimed in claim 46, wherein said unwanted computer program is a computer virus.

48. (original) A reporting computer as claimed in claim 45, wherein said requested data is a description of said event.

49. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

50. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

51. (cancelled)

52. (previously presented) A reporting computer as claimed in claim 45, wherein said reporting computer collates report data specifying one or more events that is sent together from said reporting computer to said receiving computer during said fetch of said requested data.

53. (original) A reporting computer as claimed in claim 45, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

54. (original) A reporting computer as claimed in claim 45, wherein said reporting computer and said receiving computer communicate via an internet link.

55. (original) A reporting computer as claimed in claim 45, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

56. (previously presented) A receiving computer operable to receive a report of occurrence of an event from a reporting computer, said receiving computer comprising:

a data request receiver operable to receive a request for requested data from said reporting computer;

a data provider operable to provide said requested data to said reporting computer; and

a report receiver operable to receive report data identifying said reporting computer and said event from said reporting computer during providing of said requested data to said reporting computer;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving computer.

57. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing an unwanted computer program.

58. (original) A receiving computer as claimed in claim 57, wherein said unwanted computer program is a computer virus.

59. (original) A receiving computer as claimed in claim 56, wherein said requested data is a description of said event.

60. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

61. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

62. (cancelled)

63. (previously presented) A receiving computer as claimed in claim 56, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

64. (original) A receiving computer as claimed in claim 56, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

65. (original) A receiving computer as claimed in claim 56, wherein said reporting computer and said receiving computer communicate via an internet link.

66. (original) A receiving computer as claimed in claim 56, wherein said report data includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer; and

an action taken by said reporting computer upon detection of said event; and

a checksum of a file that triggered said event.

67. (previously presented) A computer program product as claimed in claim 1, wherein said report data includes:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;

an identifier of an event type detected by said reporting computer;

an action taken by said reporting computer upon detection of said event; and
a checksum of a file that triggered said event.

68. (previously presented) A computer program product as claimed in claim 1, wherein said internet URL includes a name of a script running on said receiving computer and encrypted report data.

69. (previously presented) A computer program product as claimed in claim 68, wherein said script decrypts said encrypted report data.

70. (Previously presented) A computer program product as claimed in claim 1, wherein said report data includes an identifier of a driver triggered during said event.

71. (previously presented) A computer program product as claimed in claim 70, wherein said identifier of said driver is mapped to an identity of a virus that triggered said event.

72. (previously presented) A computer program product as claimed in claim 1, wherein said URL is not displayed on said reporting computer.

73. (previously presented) A computer program product as claimed in claim 72, wherein said URL is in the form of a hypertext link that is associated with a description of said event.

74. (previously presented) A computer program product as claimed in claim 73, wherein selection of said hypertext link results in a URL request being passed to said receiving computer.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P459/01.021.01).

Respectfully submitted,

By: ______________________ Date: 11/13/06

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660